

**BEFORE THE  
FEDERAL COMMUNICATIONS COMMISSION  
WASHINGTON, D.C. 20554**

In the Matter of:

Call Authentication Trust Anchor

WC Docket No. 17-97

**COMMENTS OF TELCORDIA TECHNOLOGIES, INC. D/B/A ICONECTIV**

Telcordia Technologies, Inc.,<sup>1</sup> doing business as iconectiv (“Telcordia” or “iconectiv”), is pleased to submit these comments responding to the Federal Communications Commission’s (“FCC” or “Commission”) questions raised in its Notice of Inquiry (NOI) on the governance role and public policy considerations related to ATIS/SIP Forum joint taskforce proposals driving toward implementing authentication for telephone calls.<sup>2</sup> iconectiv takes note of the thoroughness of the questions in this NOI and appreciates the opportunity to provide comment from a technical and operational perspective.

iconectiv has been an authoritative partner of the communications industry for more than thirty years. A U.S. based company, iconectiv has been a major architect of the United States’ telecommunications system since it was formed at the divestiture of AT&T. We have first-hand

---

<sup>1</sup> Since February 14, 2013, Telcordia has been doing business as iconectiv.

<sup>2</sup> *In the Matter of Call Authentication Trust Anchor*, Notice of Inquiry, FCC No. 17-89, WC Docket No. 17-97, rel. July 14, 2017 (NOI).

knowledge of the intricacies and complexities of creating, operating and securely evolving the country's telecommunications infrastructure and services, including the dynamic nature of telephone numbers and how they are used by the varied stakeholders in the industry. Our core critical infrastructure competencies include highly scalable industry database management, numbering services, third-party authentication, and network fraud prevention for the telecommunications industry.

## DISCUSSION

iconectiv has been an active participant in the ATIS / SIP Forum IP NNI work to verify Caller ID and authenticate calls transported over IP networks using SIP. In addition to contributing substantial foundational work behind the SHAKEN framework (Phase 1), iconectiv has been a leader in development of the specifications for the Governance Model and Certificate Management for SHAKEN (Phase 2). The breadth and depth of our industry experience, our active contribution to the SHAKEN call authentication standards, and our appreciation of the varied needs of all industry stakeholders, form the basis for our comments on the NOI.

**The Commission's Role in Advancing Call Authentication (§ 14).** The FCC asks what it should do to promote the adoption and implementation of authentication frameworks, including SHAKEN/STIR. The standards described have been developed through an open, consensus-based industry-driven process. As noted by ATIS, the standard recognizes the importance of the National Regulatory Authority (NRA), in this jurisdiction the FCC, designating a Governance Authority (GA).

FCC mandates are not required to further the adoption and implementation of the SHAKEN call authentication framework. We note current FCC rules that require the passing, where already present, of Caller ID and SIP header information, throughout the call path (See Rule 64.1601). It should be technically possible to include these SIP extensions in the rules if not already addressed. We further note that the Commission already engages in enforcement against illegal robocalling and spoofing. We believe the capabilities provided by the SHAKEN/STIR standards will enhance the Commission's current ability to identify abusers and determine appropriate enforcement action.

Furthermore, there is a significant need to educate the broader industry and the public regarding this initiative and the potential to present calls showing that Caller ID has been validated. Consumers may form certain expectations about validated Caller ID, thus the Commission has a role in facilitating the evolution of SHAKEN to support additional call originators not covered in the initial framework. SHAKEN will likely roll out network by network which provides opportunity for it to evolve and include all stakeholders over time.

Regarding the ability to move SHAKEN forward without depending on formal government mandates, iconectiv is aware of a number of precedents that operate successfully today that did not depend on such government mandates. The ATIS International Mobile Subscriber Identity (IMSI) Oversight Council (IOC), where iconectiv has served as Chair and also as Administrator for many years, is an ongoing example and allows US operators to support international roaming. In more recent years, and closer to the consumer protection domain, the FCC Technological Advisory Council (TAC) formed the Mobile Device Theft Prevention (MDTP) working group, in which iconectiv was an active contributor, comprised of cross-

industry stakeholders including mobile operators, handset makers, law enforcement, the CTIA, as well as security application providers and other industry vendors like ourselves. This evolved into an industry-led and widely adopted voluntary commitment to improve handset security and deter smartphone theft. This effort has resulted in great progress, including, among various improvements, consistency in the minimum standards for smartphone security that are also enabled when shipped, and the implementation of a nationwide Stolen Phone Checker<sup>3</sup> that helps consumers, businesses and law enforcement agencies check the status and authenticity of mobile devices to see if they have previously been reported lost or stolen. This information portal is managed by CTIA with ongoing guidance from the Commission and collaboration within the TAC MDTP working group.

**Milestones and Metrics (§ 15).** The FCC seeks comment on metrics that should be used to measure the progress of adoption. Metrics are a work item assigned to the multi-stakeholder ATIS Packet Technologies and Systems Committee (PTSC). This group is expected to make recommendations this year. If the Commission allows this specification work to be completed and be instrumented in the networks, it should enable a data-driven approach to determining key areas for attention in the evolving call authentication framework.

The FCC also asks about entities that could delay or impair the implementation framework, and how to mitigate the risks. It is a fact that network equipment has the ability to break SIP headers and compromise the continuity of information in the end to end call signaling flow. This would impair the effectiveness of the framework. However, enforcement of rules such as not permitting interference with these SIP extensions can prevent this problem.

---

<sup>3</sup> [www.stolenphonechecker.org](http://www.stolenphonechecker.org)

**Existing Barriers (§ 16).** The FCC solicits input on those factors that prevent or discourage stakeholders from developing, implementing, or deploying authentication frameworks. Operationally, as the framework rolls out, it relies on the integrity and/or rigor of the originating network attesting to the integrity of the Caller ID. Terminating networks must trust correct cryptographic signatures and advise their customer of verified Caller ID if they are complying with the framework specification. Thus the overall solution must include prompt investigation of originations that are found to be illegally spoofed yet still have authenticated Caller ID such that identification of entities who misuse their certificate(s) can be conveyed to the PA who maintains the list of parties eligible to sign calls within the SHAKEN framework. Entities originating voice traffic will need to invest in technology and operations in order to participate in the SHAKEN framework. This might be a factor for some stakeholders.

**SHAKEN/STIR Framework (§ 17).** The FCC asks if the SHAKEN/STIR frameworks are the appropriate ones for call authentication on SIP-based networks, and if there are other alternatives. SHAKEN/STIR has been developed with substantial industry input, reflecting the current consensus and leveraging long proven techniques for conveying untampered information via cryptographic signatures using public/private key pairs. This industry framework has also addressed a weakness in some PKI implementations where any party could create their own certificates and self-attest to their trustworthiness. This is a key component providing SHAKEN/STIR with operational integrity and any alternatives would need to address this factor. Nonetheless, there may be other viable mitigation techniques, and these mitigation techniques can co-exist productively with SHAKEN/STIR. The SHAKEN/STIR industry specifications acknowledge and refer to other potential approaches that could be incorporated. iconectiv

supports the perspective that the immediate need is to launch this framework and gain real operational experience that can drive the roadmap.

**Governance Authority and Policy Administrator (§ 18-20).** The FCC asks whether the GA and Policy Administrator (PA) functions should be merged and operated by a single authority. iconectiv does not see a necessity for a combined entity and, more fundamentally, sees these two roles as very different. The GA defines guidelines and requirements for the framework, ideally using a multi-stakeholder forum and consensus driven approach while the PA is an operational entity whose role is to administrate the mechanisms defined to ensure trustworthiness in the use of the public/private key pairs. The Commission further inquires about mechanisms for interactions between the two entities. Being an operational entity, the PA should be accountable to the GA, adhere to the established service level agreement (SLA), report ongoing metrics as well as actively contribute to this multi-stakeholder forum.

The FCC also seeks comment on what entity would best serve as the governance authority and what entity would best serve as the policy administrator. A well-respected, industry-led organization would be a very suitable entity for the FCC to support or designate as GA. ATIS, for example, with more than 30 years of standards leadership encompassing all sectors of the ICT space, including such critical elements as the 911 National Emergency Address Database, and representing America's 5G requirements globally,<sup>4</sup> possesses the requisite credentials. ATIS has also taken a leading role to establish a call authentication solution that can be operationalized, looking well beyond the SIP message information elements. There may be other entities that could provide some of these functions.

---

<sup>4</sup> See <https://sites.atis.org/insights/atis-overview/>

iconectiv agrees that the GA, in turn, should be empowered to select a PA.<sup>5</sup> iconectiv shares the belief that consensus-driven, industry-endorsed criteria, determined and administered through a transparent process, would result in selection of a Policy Administrator best suited to administer certification governance and procedures. Key criteria for a PA include administrative governance and technology management expertise, evidenced by longstanding leadership in industry-wide database management and active contributions to the standards organization or other forums that govern those solutions. This is particularly important given robocalling and spoofing will be a constantly evolving threat for some time to come. In addition, expertise in network interconnection topologies and the dynamics of telephone number usage, as well as a strong cybersecurity posture resilient to compromise would be among the desirable attributes for a PA. Familiarity and experience with the industry process for OCN vetting and assignment is also a valuable credential in the initial phases of PA implementation. There is also a sense of urgency to consider, as the Commission's robocall mitigation goals place a premium on rapid implementation. The PA should demonstrate the operational experience and expertise to quickly implement the specified procedures and workflows to advance public policy goals.

In paragraph 19, the Commission asks whether GA/PA governance “choices and trade-offs depend on whether certificates are issued for specific telephone numbers (or number blocks), or whether a single certificate is issued for each service provider?” SHAKEN certificates are obtained on a company or entity basis, and are initially allocated to Service Providers (SP), rather than telephone numbers (TNs). TN-based certificates would significantly complicate this framework given the massive volume and highly dynamic nature of TN ownership and usage. It is difficult to maintain the chain of custody of a TN and its respective

---

<sup>5</sup> ATIS ex parte in CG Docket No. 17-59, Tom Goode letter and presentation, June 30, 2017, slide 11.

certificate with the service or entity that originates traffic using that TN. Thus, it would be overly complex to govern and control trust at scale if SHAKEN used TN-based certificates. TNs are resold to other parties including cloud communication providers and many other innovators. They are assigned to enterprises who may originate calls with said TNs across their infrastructure for least cost routing purposes or customer convenience regardless of the serving carrier or they may delegate the originations to contact center providers who select a Caller ID on their behalf as operational policies dictate.

Furthermore, iconectiv suggests this adds unnecessary complexity. The SHAKEN framework follows some key principles in pursuit of Caller ID authentication, namely:

- There will be attestation performed by the originating network for IP-based calls to US phone numbers,
- This attestation can identify the Caller ID and the entry point into the US network,
- Full attestation of the Caller ID will be based on the originating network's local policy regarding how the network determines this is a legitimate use of the Caller ID at this particular time and on that particular 'circuit',
- The attestation will be cryptographically signed to ensure end-to-end integrity,
- Abuse will be detected, traced back and dealt with and offenders risk losing the privilege to attest to their calls and potential additional enforcement action.

These principles deliberately rely on a trust model that the entities given certificates to attest to their call originations will behave with rigor. This will not be a perfect solution, given



the dynamic and evolving use of TNs noted above, making traceback, investigation and enforcement very important components of the overall scheme. This deployment experience will enrich industry knowledge about the evolving techniques related to infrastructure and TNs that will be used by adversaries who continue robocalling and spoofing. These learnings provide for fact-based insight to drive the industry's priorities and roadmap.

While iconectiv believes an OCN-level certificate as the initial industry approach would be efficient and effective for call authentication, we also appreciate that this could disadvantage non-OCN stakeholders such as resellers, innovators, enterprises and such who might not see all their legitimate calls fully attested to. The industry discussions to date recognize this issue and are actively exploring solutions to this challenge. Operationally, the rollout for SHAKEN is likely network by network and the early operational learnings will be important to help the industry to evolve the framework to support these broader stakeholders.

**Extending Numbering Administration to the PA (§ 21-24).** The FCC asks about the benefits and drawbacks of designating one of the entities currently engaged with existing numbering administration authority for the PA role. iconectiv cautions that there are limited synergies between the PA functions and most numbering administrators so an answer to that question is best not generalized. The ongoing entity eligibility vetting processes and broad notification to the industry, at the core of the PA's responsibilities, are distinctly different from numbering administrators. Numbering responsibilities revolve around managing blocks/pools of numbers and tracking their assignments and re-assignments, reporting on the utilization of this scarce resource. The required vetting and subsequent notification to industry is handled by other numbering oriented entities. An exception to this might be the Local Number Portability

Administrator (LNPA) where eligibility and notification play strongly. However, as stated above, assignment of TN-based certificates is challenging and there is far more than number porting behind that complexity.

There is also the need to allocate time and resources to ensure specifications and change orders are fully in line with industry direction and timing, as well as costed appropriately. This, however, may also inhibit rapid implementation and ongoing evolution compared to an industry-led and market driven model. One thing is certain, the illegal spoofers – whether spammers or, worse, fraudsters – will not sit still and the industry will need to be poised to adapt and even anticipate such highly motivated and technically proficient adversaries.

**Alternative Means (§25-26).** The FCC seeks comment on alternative means of call authentication. As stated in response to ¶ 17, iconectiv believes that SHAKEN is technically and operationally workable and could evolve to support a broader set of call authentication mechanisms.

With regards to alternatives, the SHAKEN Trust Authority model is similar to an inter-domain Public Key Infrastructure (PKI). With SHAKEN, the PA is external to the PKI and serves as the Trust Anchor that maintains a list of trusted CAs on behalf of the relying parties in the PKI. This mechanism prevents self-signing of certificates without proper oversight and is key to the SHAKEN framework. Each authorized CA, in turn, must support the Certificate Policy (CP) as established by the PA, and the PA is responsible for reviewing and approving the Certification Practice Statement (CPS) as provided by the CA to ensure compliance.

For any approach to authenticated calls, it will be critical to ensure that there are eligibility criteria to participate and that all participants are kept informed of who is eligible. The SHAKEN GA and PA are designed to ensure there are clear policies and mechanisms to administrate them on an ongoing basis.

**CA Criteria (§ 29).** The FCC seeks comment on two proposed criteria, previously suggested by ATIS for CAs, sufficient certificate management expertise and incorporation in the United States. Given the limited scale of certificate issuance for a SHAKEN CA and the well-established technological and operational requirements behind that, certificate expertise may not be as important as other factors. iconectiv suggests that it is perhaps just as, if not more, critical for any CA to possess sufficient telecom domain knowledge to understand the nuances of our complex industry. This would include such considerations as IP and TDM call flows, network interconnection including tandems, multi-homing and other topological factors, as well as TN dynamics such as reselling, pooling and porting. Implicit in all this is the proven ability and inclination to contribute this body of knowledge to the industry forum striving to evolve the criteria for and approach to certificate issuance to a broader set of constituents as noted in response to § 19. In addition, with the prevalence of bad actors who continuously innovate and refine their techniques, any CA must demonstrate proven cybersecurity capabilities.

**Criteria for SP Validation (§ 30).** The FCC asks whether OCNs are a reliable criterion for assuring that a carrier is eligible to sign calls. iconectiv believes the industry's consensus position, reflected in the Phase 2 ATIS standard (ATIS-1000080) is reasonable, *i.e.*, that carriers have an OCN (Operating Company Number) in order to sign calling-party information. OCNs

are used in mechanized systems throughout the industry to facilitate the exchange of information according to various ATIS standards and there is a formal process and criteria for assignment of an OCN which is well-documented by NECA (the National Exchange Carrier Association), and span the various types of Service Providers (listed below).

In accordance with the Alliance for Telecommunications Industry Solutions (ATIS) Industry Numbering Committee (INC), where iconectiv is a co-Chair, only the following Company Code categories are permissible for direct assignment of numbering resources (CO codes, thousands-blocks, 5XX-NXX, 9YY-NXX and p-ANI) from NANPA or the Pooling Administrator:

• Incumbent Local Exchange Carrier	ILEC
• Regional Bell Operating Company	RBOC
• Competitive Local Exchange Carrier	CLEC
• Personal Communications Service	PCS
• Unbundled Local Exchange Carrier	ULEC
• Wireless Carriers	WIRE
• Internet Provider Enabled Services	IPES (only permitted with an FCC waiver)

NECA specifies the documentation required to obtain an OCN.<sup>6</sup> As the Telecom Routing Administrator for the North American numbering plan and longstanding Chair of ATIS TMOC, iconectiv is intimately familiar with the standard industry processes that depend on an OCN for participation and we believe that extending this to SHAKEN is appropriate for the initial criteria to determine which entities a CA can service. As stated earlier, iconectiv acknowledges that this could disadvantage non-OCN stakeholders initially, but believe the industry could leverage

---

<sup>6</sup> See *Required Documentation* <https://www.neca.org/PublicInterior.aspx?id=1947#RequiredDocumentation>

SHAKEN operational experience as it evolves the framework to the broader set of call originators and support non-OCN stakeholders.

**Scope of Certificate Coverage (§ 31).** The FCC solicits input on whether certificates should cover certain carriers, or could also cover specific TNs or ranges of TNs. Certification at the carrier level allows for the most efficient use of existing governance structures. Furthermore, as noted in response to § 19 above, striving to stay aligned in real-time with the chain of custody of a TN and the topology of a call origination is very challenging and likely not practical as a means to determine who can legitimately use a certificate for a given call origination. SHAKEN depends on trust between all entities privileged to sign call originations and ongoing privilege is predicated on good behavior. This trust model will continue to be important to scale eligibility when and if extended to additional call originators such as enterprises, contact centers, cloud communication providers, and others. To reduce time-to-implementation, iconectiv recommends that the proposed SHAKEN model should be utilized before assessing alternative methods, e.g., number ranges, because to do otherwise could significantly slow industry implementation.

**IETF Certificate System Enrollment Options (§ 34).** The FCC seeks comment on the various IETF alternatives for enrollment in the certification system. As noted above, a method that focuses initially on Service Provider deployment is faster to implement and would facilitate quicker achievement of the Commission's goals for robocall mitigation. The key question remains "why is this use of Caller ID legitimate for this particular call such that it should be fully attested to?" This is a very difficult question to answer with certainty for all originations, so detecting and addressing abuse has to be a key principle as a protective backstop to the scheme. This will continue to be key as the solution scales to additional industry stakeholders.

With regards to the specific FCC question regarding the feasibility of a certificate delegation approach, this is being explored by ATIS and the industry contributors to SHAKEN. This can be complex as it may depend on additional network gear implementing SHAKEN certificates and new operational processes to ensure that this extended eligibility is used with integrity. iconectiv is confident that ATIS and the industry will ultimately address this but recommends proceeding with the current approach in the interests of time while working in parallel to extend the scheme in a thoughtful manner with due haste.

**Valid Types of Authentication and Verification Service Providers (§ 35).** The FCC seeks comment on allowing different types of entities and devices to provide authentication and verification services. SHAKEN was developed as a complement to STIR because it was recognized that the complexity of synchronizing signatures and managing credentials at the device level, in the network, was extremely challenging. Further, it is worth considering that the majority of robocalls and spoofed calls are coming into the network via international trunks and domestic wholesale trunks. As such, looking at other constituents, such as devices, to authenticate or verify calls may not address a real problem. Extending SHAKEN to additional constituents could be based on operational experience, with the resulting fact-based data useful to help set future priorities.

**ACME and Alternatives (§ 36).** The FCC asks if replacements or interim solutions should be considered as the IETF continues work on the ACME protocol. As the FCC notes, ACME is still in the process of development, and leeway might be given to allowing other certificate management environments to be within scope of the Phase 2 Governance standard. Within the SHAKEN standards, implementation of ACME is not mandatory. During the

development of SHAKEN, it was industry consensus that the ACME protocol was best capable of providing the needed functionality. Nevertheless, there is nothing that prevents vendors from utilizing other protocols that provide similar functionality as ACME. In fact, alternative schemes can coexist, and entities originating calls could be free to choose the most suitable for their needs. As noted previously, iconectiv suggests that the most important consideration for any alternatives would be adherence to procuring certificates from eligible CAs and assigning them to eligible carriers or other entities as identified by the PA in accordance with the industry standard.

**IP vs. TDM Scope (§ 39).** The Commission asks several interdependent questions around progressing work on IP-based voice telephony in contrast to legacy signaling systems, including whether advancing authentication of IP-based calls can alleviate illegal robocalling regardless of whether TDM authentication solutions exist. It was for good reasons that the FCC and industry had agreed that the STIR/SHAKEN standard and implementation framework apply to the cryptographic authentication and verification of telephone numbers associated with calls traversing Internet Protocol (IP) voice networks.<sup>7</sup> iconectiv appreciates the challenges in evolving the TDM domain and fully supports that perspective.

iconectiv co-chaired the recent CSRIC V Working Group 10 which studied the vulnerabilities in TDM/SS7 networks. This WG identified the evolving threats to the SS7-based infrastructure and the critical need to continue the enhancement of existing controls to combat service integrity attacks. It was also determined that the SS7 User Part protocols that convey call setup information could not be changed with new security features, including cryptographic

---

<sup>7</sup> Industry Robocall Strike Force Report, April 28, 2017, pp. 4-5.

signatures, because of the extensive and aged embedded base. The WG recommended security best practices including enhanced filtering of signaling messages across interconnection boundaries and other controls. This included “intelligent” controls to perform advanced data analytics to detect “signs” of attack in terms of changing subscriber profiles, fraud and unauthorized location tracking. Applying analytic techniques to calling patterns may help detect and prevent robocalls but would not ensure the integrity of the Caller ID in itself.

We do note separate efforts to improve the display of verified Caller ID information through the ISUP screening indicator interworking.<sup>8</sup> This may enable legacy systems some progress combatting spoofing but should not encumber SHAKEN in pursuit of a unified IP/TDM solution.

**International Issues (§ 40).** The FCC seeks comment on the effect of authentication frameworks on spoofing and robocalls originating in other countries. The implementation of the SHAKEN framework will provide a level of attestation to the called party on incoming international calls. It has yet to be decided how that will be displayed on the handset, but the call will certainly not have full attestation initially. An unintended consequence could be that international calls do not get answered by US subscribers if they decide not to answer calls with unverified Caller ID. These subscribers may incur the, otherwise avoidable, cost of international rates should they determine afterwards that this was legitimate and decide to return the call.

Nevertheless, with the capabilities of SHAKEN, the call can be traced back to the international gateway where it entered the US which can help curtail abuse and eventually legitimate calls may support full attestation for Caller ID within this framework. As to the

---

<sup>8</sup> Industry Robocall Strike Force Report, April 28, 2017, p. 9.



implications to international agreements and obligations, similar to iconectiv comments on ¶ 14 regarding tandem topologies, at a minimum, international wholesale carriers and the international long distance operators (ILDOS) handling traffic between the originating and terminating jurisdictions should convey the SHAKEN SIP extensions transparently if the solution is to work end to end. Given the concentration of international originations in robocalls and spoofing, iconectiv believes it is a worthy goal for ATIS and the FCC to work with global stakeholders to evolve SHAKEN into a scalable international system against misuse of the telephone network. With our global footprint and regulatory relationships, iconectiv can certainly contribute constructively to that objective.

**Authentication Service (STI-AS) as a Privacy Service (¶ 43).** The FCC seeks comment on the suitability of an authentication service also acting as a privacy service. Conceptually, an authentication service could vouch for the integrity of caller without explicitly conveying the Caller ID to the called party such as done with call management solutions designed for anonymity between one or both parties. This could be considered incorporating a privacy service into the evolution of SHAKEN authentication services. Similarly, Caller ID blocking solutions might leverage SHAKEN to distinguish proper Caller ID blocking from adversaries attempting to hide behind that service, especially as SHAKEN succeeds over time and opportunities for abuse become few and far between.

**Security Considerations (¶ 44).** The FCC seeks comment on the effects of an authentication mechanism on security of networks, consumers and carriers. iconectiv notes that the SHAKEN Phase 2 Governance Model and Certificate Management specification was

engineered to take a wide range of security considerations into account. The design and carefully defined processes and flows serve, among other goals, to ensure security.

The CSRIC WG 10 recommendations recognized that there were common elements with the SHAKEN/STIR framework including the 3GPP circles of trust concept among service providers, and securing network elements and subscriber and network data. Even if the SHAKEN/STIR framework is implemented properly, rigorous lifecycle management is required to secure new “trusted” network authentication and integrity functions and interfaces and to accurately profile subscriber traffic to avoid unintended denial-of-service situations. A robust intrusion detection capability will also be needed with all SHAKEN components to identify compromises and other security incidents, given this well publicized framework will become a target of adversaries across the globe.

Specific to SHAKEN, there are several security aspects of the framework that merit attention: The authentication and verification service’s visibility into Customer Proprietary Network Information (CPNI) regarding who is calling whom and at what time of day, drives a need for rigorous data loss prevention practices and the requirement for companies to have a strong cybersecurity posture. Key management tools used by carriers and the private keys they use in their authentication service must be closely guarded as with any X.509 scheme. For the PA, industry mechanisms controlling eligibility data and process flows for certificate issuance and acquisition must be secured throughout the lifecycle from identification and registration of eligible entities through incident prevention, detection, response and ultimately recovery in the case of compromise. For CAs, their creation and distribution of certificates should be tightly controlled and align to well defined best practices such as those in the National Institute of

Standards and Technology (NIST) Special Publication SP800-57 series<sup>9</sup> on cryptographic key management guidance for defining and implementing appropriate key management procedures, using algorithms that adequately protect sensitive information, and planning ahead for possible changes in the use of cryptography. All of the SHAKEN component providers should have experience using a robust cybersecurity program to protect the confidentiality, integrity and availability of the solution such as the NIST Cybersecurity Framework (CSF)<sup>10</sup>. Consistent with the above, components should also apply the security principles of least privilege and defense in depth, as well as maintain solid audit trails to assist with timely investigations on suspected abuse.

## CONCLUSION

iconectiv commends the Commission for launching this proceeding to build a record on the diverse considerations at hand and we appreciate the opportunity to provide technical and operational input based on our experience. The SHAKEN/STIR governance model is the product of industry consensus and demonstrates a collective motivation to solve this serious problem plaguing all consumers. The proceeding enables the FCC to make an informed determination regarding what is appropriate to mandate from a regulatory perspective versus endorse as a voluntary industry framework that can respond in an agile manner to what is clearly an advanced persistent threat in cybersecurity terms. iconectiv encourages the Commission to support and facilitate timely deployment of SHAKEN to allow for operational experience that

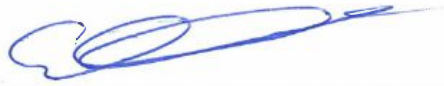
---

<sup>9</sup> <http://csrc.nist.gov/publications/PubsSPs.html>

<sup>10</sup> <https://www.nist.gov/cyberframework>

can drive a roadmap addressing the varied call types and call originators in the industry. In this manner, call authentication can be established at scale and extended, and moreover, flexibility can be maximized so that, as the FCC intends, all sectors of the telecom ecosystem can work together to combat the evolving robocalling and spoofing threat.

Respectfully submitted,



---

*Chris Drake*  
*CTO of Telcordia Technologies, Inc. d/b/a iconectiv*

Dated: August 14, 2017